

## UNITED STATES DISTRICT COURT

for the  
Southern District of OhioFILED  
RICHARD W. NAGEL  
CLERK OF COURT

6/22/22

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
AN ACCOUNT WITH THE CLOUD SERVICE  
PROVIDER MICROSOFT AZURE

Case No. 3:22-mj-196

U.S. DISTRICT COURT  
SOUTHERN DIST. OHIO  
WEST. DIV. DAYTON

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

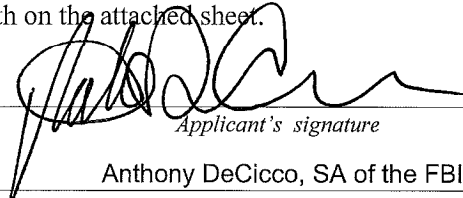
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1030(a)(2)(C)	unauthorized access to a computer system
18 U.S.C. § 1030(A)(5)(a)	unauthorized damage to a protected computer system

The application is based on these facts:

See Attached Affidavit of Anthony DeCicco

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Anthony DeCicco, SA of the FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: June 22, 2022

City and state: Dayton, Ohio



Caroline H. Gentry  
United States Magistrate Judge



IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH THE  
CLOUD SERVICE PROVIDER  
MICROSOFT AZURE FOR ACCOUNT:  
chrisk[@]lac.authenticom.com AND  
AZURE ACTIVE DIRECTORY ID: 501d2bc4-  
5948-40e9-ad5e-f1f4ee3718f2, 91845580-  
9c09-41e0-82fa-feec820216ed, a0285d75-  
854d-4fde-9e8e-45c3d2800285, 78807487-  
964f-4c90-8647-e55ce75705a7 and  
74b34da8-d8b7-  
423a-af50-e5b27cce2d5f

3:22-mj-196

Case No. \_\_\_\_\_

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Anthony DeCicco, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with cloud service assigned with chrisk[@]lac.authenticom.com and Azure Active Directory ID: 501d2bc4-5948-40e9-ad5e-f1f4ee3718f2, 91845580-9c09-41e0-82fa-feec820216ed, a0285d75-854d-4fde-9e8e-45c3d2800285, 78807487-964f-4c90-8647-e55ce75705a7 and 74b34da8-d8b7-423a-af50-e5b27cce2d5f (“the SUBJECT ACCOUNT”), with listed subscriber(s) Authenticom LLC, or that is in the custody or control of Microsoft Corporation, a cloud service provider that is headquartered at 1 Microsoft Way, Redmond, WA 98052. As a provider of cloud services, Microsoft Corporation is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15).

2. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft Corporation to

disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been since October 2019. I am currently assigned to the Cincinnati Field Office, Columbus Resident Agency, Cyber Crime Squad, which is responsible for investigating computer and high-technology crimes. During my career as an FBI SA, I have participated in numerous cyber-related investigations. During the investigation of these cases, I have participated in the execution of numerous arrests, search warrants, and seizures of evidence. Since my assignment to the Cyber Crime Squad, I have received both formal and informal training from the FBI regarding cyber investigations. I am trained and authorized to investigate the offenses alleged herein. Prior to working with the FBI, I received a Master of Science in Computer Information Systems and cyber security from Boston University. I have also completed the SANS Institute GIAC Security Essentials (GSEC) and GIAC Certified Incident Handler (GCIH) courses.

4. The facts in this affidavit come from my personal observations, training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1030(a)(2)(C) (unauthorized access to a computer system) and 1030(A)(5)(a) (causing the transmission of a program, code or command that causes unauthorized damage to a protected computer system) have been committed by Authenticom

LLC, and as-yet unidentified co-conspirators. There is also probable cause to search the information described in Attachment A for evidence of these crimes as further described in Attachment B.

### **JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

#### **Overview**

7. In or around March 2020, Reynolds and Reynolds (the VICTIM), located at 1 Reynolds Way, Building 2, Kettering, OH 45420, approached FBI Cincinnati Division with the allegations of a persistent computer intrusion into the VICTIM’s proprietary system, known as a Dealership Management System (DMS), by Authenticom LLC (the SUBJECT COMPANY).

8. The DMS was designed by the VICTIM to provide their customer base with a system to facilitate the daily operations of running an automotive dealership. For example, the system creates a network of databases delineated based on the roles of the dealership employees. From customer financials and purchase history, all are interfaced through the DMS.

9. The VICTIM took measures to protect and secure the data maintained on the DMS. The DMS required the creation of different account roles with varying levels of privilege. For example, a dealership automotive repair mechanic’s account would not have access to the financial data of the DMS.



10. Over the years of operation, the VICTIM experienced atypical network behavior from select dealerships. The VICTIM alleged large volumes of data had been leaving their network and the data was unaccounted and exposed to the internet. The VICTIM noticed the export of data was likely automated, due to observed behavior of large regular interval exports.

11. The VICTIM took measures to prevent the exporting of data outside of the DMS such as, contractually prohibiting dealerships from divulging their password with third-party entities. From a technical perspective, the VICTIM limited the amount of data capable of being exported from the DMS at any given time and implemented security measures such as Completely Automated Public Turing test (CAPTCHA) challenges prior to export, and software designed to detect other types of computer automation. After some time and the implementation of the security measures, the unauthorized data exports continued. Based on information from the VICTIM company, the unauthorized data exports are ongoing and have continued into 2022.

12. In 2018, the SUBJECT COMPANY filed an anti-trust lawsuit against the VICTIM. The SUBJECT COMPANY's lawsuit alleged the VICTIM had a monopoly on the automotive DMS industry. During the discovery phase of the lawsuit, the VICTIM discovered the alleged involvement of the SUBJECT COMPANY in the improper accessing of the VICTIM's computer system and data.

13. According to depositions and items obtained via discovery in the DMS Antitrust Litigation of 2018 from the Northern District of Illinois Eastern Division, the SUBJECT COMPANY was alleged to have been scraping, referred to as "polling" by the SUBJECT COMPANY, data from the VICTIM DMS to create their own similar DMS system called DealerVault.

14. Analysis by the VICTIM of the discovery material included details for a complex system of processes used to circumvent DMS security measures. For example, the SUBJECT COMPANY allegedly used, “CAPTCHA farms”, or the outsourcing of CAPTCHA challenges to groups of overseas individuals whose sole daily job was to answer CAPTCHA challenges; and the process of “menu walking”, or the use of code to automate the movements of a user interfacing with the DMS in attempt to circumvent automation detection features of the DMS. Additionally, the material showed correspondence between the SUBJECT COMPANY requesting elevated privileged access from the dealership to access all parts of the DMS. Notably, based on information from the VICTIM, the VICTIM has never provided the SUBJECT COMPANY with complete access to the DMS system or authorized it to extract data from the DMS system. Based on my training and experience, as well as my familiarity with the facts of this case, I know that the DMS generates logs that track the access to its data, including the volume, time, number of events, and network protocol used. Based on my training and experience, I know that, when individuals improperly access a protected computer system like the DMS and remove data from it, they will manipulate (e.g., delete) logs such as the ones described above in an attempt to conceal the intrusion.

15. Access points to the DMS were determined to be through the VICTIM’s customers – i.e., dealerships’ network infrastructure. Upon interview of the Information Technology administrator and review of logs voluntarily provided by one of the dealerships, a computer at the dealership with the domain name: JAY-DSK-010 was discovered as containing the SUBJECT COMPANY’s proprietary software. Based on a review of discovery from the anti-trust litigation, I know that the SUBJECT COMPANY’s proprietary software is one of the tools that it uses to improperly access data from the VICTIM’s DMS system. The logs also

showed that the dealer's computer was communicating with (i.e., receiving commands from, and sending data to) IP addresses associated with Microsoft Azure.<sup>1</sup> Based on my training and experience, this pattern of activity would be consistent with some type of system located on Microsoft Azure giving instructions through the dealer's computer to improperly pull data from the DMS and then transfer it back to the SUBJECT COMPANY's Microsoft Azure infrastructure.

16. FBI obtained a court order requiring Microsoft Azure to produce records and logs revealing the services that the SUBJECT COMPANY has acquired from Microsoft Azure. Based on my review of these records, as well as my training and experience, I conclude that the services that the SUBJECT COMPANY has acquired from Microsoft Azure would be consistent with the infrastructure required to remotely and improperly access the VICTIM DMS by the SUBJECT COMPANY. Based on information from Microsoft Azure, the infrastructure is located in chrisk[ @ ]lac.authenticom.com and Azure Active Directory ID: 501d2bc4-5948-40e9-ad5e-f1f4ee3718f2, 91845580-9c09-41e0-82fa-feec820216ed, a0285d75-854d-4fde-9e8e-45c3d2800285, 78807487-964f-4c90-8647-e55ce75705a7 and 74b34da8-d8b7-423a-af50-e5b27cce2d5f ("the SUBJECT ACCOUNT"). Inspection of the content contained on in the SUBJECT ACCOUNT will provide the FBI with the ability to confirm or dispel the alleged computer intrusion conducted by the SUBJECT COMPANY. For instance, access to the

---

<sup>1</sup> Microsoft Azure is a cloud-computing services operated by Microsoft-managed data centers, for the purposes of providing Software-as-a-service, Infrastructure-as-a-service, and Platform-as-a-service. Phrased differently, a business such as the SUBJECT COMPANY can lease computing services from Microsoft Azure. The business then decides how to use those computing serves – for instance, to run a system that extracts and stores data – and Microsoft Azure simply provides the infrastructure.



SUBJECT ACCOUNT will allow FBI to search for source code that would suggest that the SUBJECT COMPANY is improperly manipulating (i.e., deleting data such deleting logs, modifying security configurations, etc.) of the DMS system or VICTIM COMPANY's computer infrastructure.

#### **Overview and Normal DMS Data Flow**

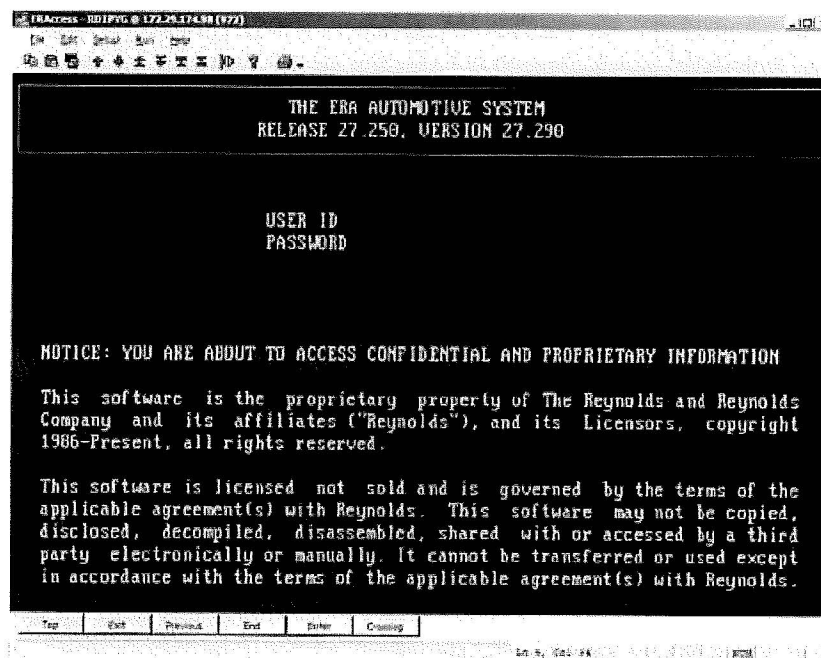
17. On or about November 23, 2020, the VICTIM demonstrated normal use of the DMS to FBI. Dealerships typically purchased two primary services for the function of the dealership, a DMS that served the primary dealership functions and 3rd party software that provided other vendor data (e.g., vehicle information from the web). The SUBJECT COMPANY promotes itself as having the ability to provide both types of vendor data and the functions of a DMS.

18. The DMS was a compilation of databases and sources physically housed in a datacenter on the VICTIM campus. The DMS was comprised of databases storing: financial data, consumer personally identifiable information, vehicle inventory, vehicle service history, service parts, appointment data, sales history, payroll data, and much more. These databases were referred to as ERA-Servers. The ERA-Servers ran on Linux distribution CentOS with some running on Unix. The ERA-Servers are controlled by a proprietary controller called the Reynolds Integration Hub (RIH). The RIH performed integrity checks on the queries submitted and parity checks on the user IDs accessing data attempting to ascertain whether the UserID was "trusted" (e.g. does the user have authorization to query the data, what is the associated serial number, does it derive from a known network address, etc.). The DMS was described as the backbone of the automotive industry.

19. An authorized license holder of the DMS, defined as someone paying for access to the DMS and bound by the VICTIM terms of service, could elect to purchase their own server/infrastructure to be housed at the dealer location, or could lease server space at the VICTIM datacenter. Once the hardware arrangement had been established, the VICTIM developed personalized software for the dealer. The personalized software consisted of variations of ERACCESS, ERA-IGNITE, or Software Manager.

20. ERACCESS was thousands of lines of pick/basic code that produced a terminal-esque environment for the user to navigate similar to what was seen in Figure 1. ERA-IGNITE was software developed with a custom Integrated Development Environment (IDE) written in C++ programming language. ERA-IGNITE software was a newer, more user-friendly interface for users. The VICTIM had begun to phase out ERACCESS, however, some dealers continued to use it.

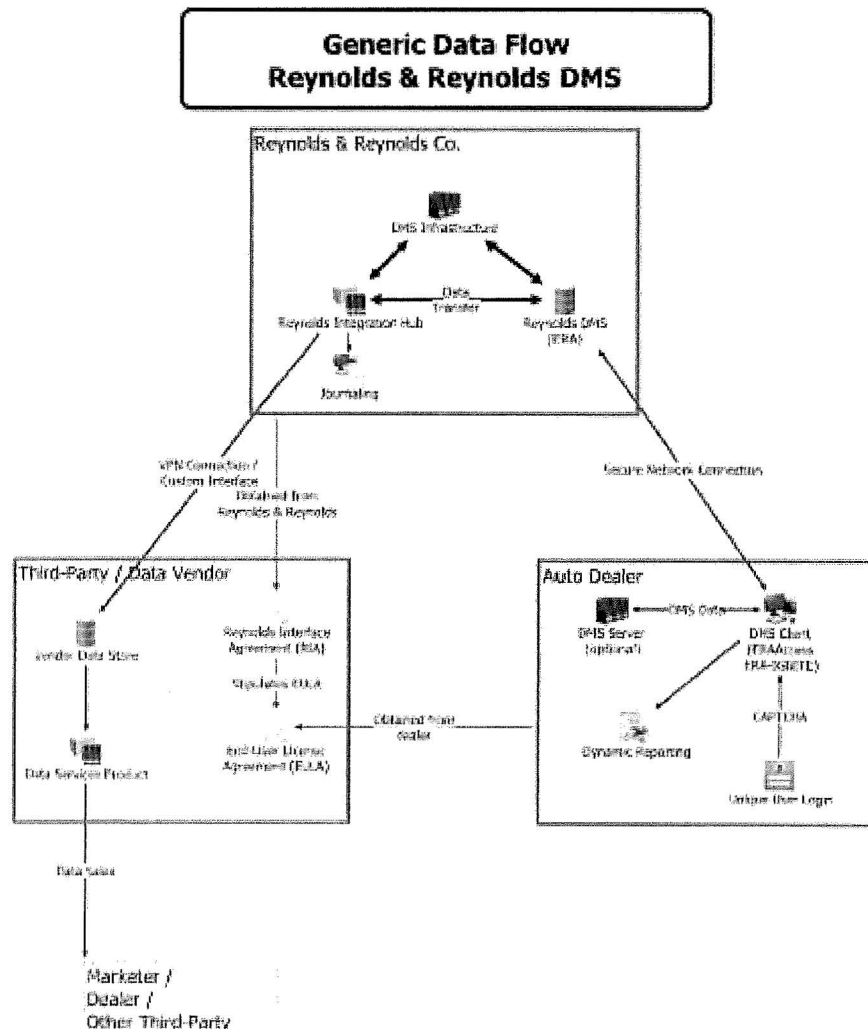
**Figure 1: Login page for ERACCESS, a Pick/Basic based program. Note the banner, which appeared on every login instance to the VICTIM DMS**





21. Software Manager provided the user with the ability to update to the latest ERACCESS or ERA-IGNITE client. All three software platforms acted as thin clients to the server and Secure Delivery Center (SDC), meaning most of the processing was conducted on the server and sent to ERA Servers via Virtual Private Network (VPN) established by the SDC. Figure 2 below depicts a high-level overview of the communication flow within a the DMS.

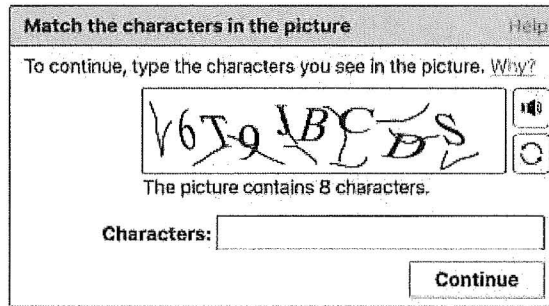
Figure 2: Data flow between a dealership and the VICTIM DMS



22. Once the dealer obtained ERA-IGNITE/ERACCESS software, they would create a User ID and password with THE VICTIM defined privileges, access and roles. As part of the VICTIM Reynolds Interface Agreement (RIA) and End-User License Agreement (EULA), the dealer was prohibited from sharing the credentials with any third parties. Once the connection between the verified user and ERA-IGNITE/ERACCESS had been established, the user was able to navigate through various menus or terminal screens to query the desired data. For ERA-IGNITE this included navigating through menus, selecting the desired database, specifying parameters for the query (e.g., between a specific date range, keyword, Boolean modifier, etc.) and running a dynamic report.

23. The dynamic report queries the corresponding ERA-Server for the requested data and populates a window with the results. The user can choose to export the data into three file types: Portable Document Format (PDF), Excel, or Comma-separated Values (CSV). However, for the export to succeed, the user must answer a challenge question. Namely, a Completely Automated Public Turing test (CAPTCHA) would appear and prompt the user to correctly answer before allowing to continue. See Figure 3 below for an example of CAPTCHA. Upon successful completion of the CAPTCHA prompt, the user is given the option to save the exported report.

Figure 3: Example of CAPTCHA question, similar to the ones used by the VICTIM DMS



#### Authenticom's Data Flow and Exfiltration Process

24. The SUBJECT COMPANY's unauthorized use of the VICTIM DMS consisted of social engineering dealers for their DMS credentials. The dealer credentials were stored on a SQL Database hosted by Salesforce or Microsoft Azure virtual servers. On a virtual server running Windows Server 2003 in Microsoft Azure, the SUBJECT COMPANY hosted a custom script, written in Pick/Basic named Polling Client Manager (PCM). The script established a Secure Socket Shell (SSH) called Authentilink, also known as DVConnect to the dealer's network. From the dealer's network, the script would programmatically input the dealer's credentials into the login prompt for either ERACCESS or ERA-IGNITE, depending on the software license purchased by the dealer from the VICTIM.

25. Upon a successful login to ERA-IGNITE by an Authenticom user, the PCM script would navigate through the DMS menus, referred to as "menu walking" by the SUBJECT COMPANY and select the desired database initially configured through the PCM by the SUBJECT COMPANY user (e.g. financial dataset, consumer history, part inventory, etc.). The script would run a dynamic report with as large of a dataset allowed by the system. The PCM script would then attempt to export the data. If a CAPTCHA prompt appeared, the PCM script would execute one of two executables, "notepad.exe" or "CaptchaSolver.exe". Notepad.exe

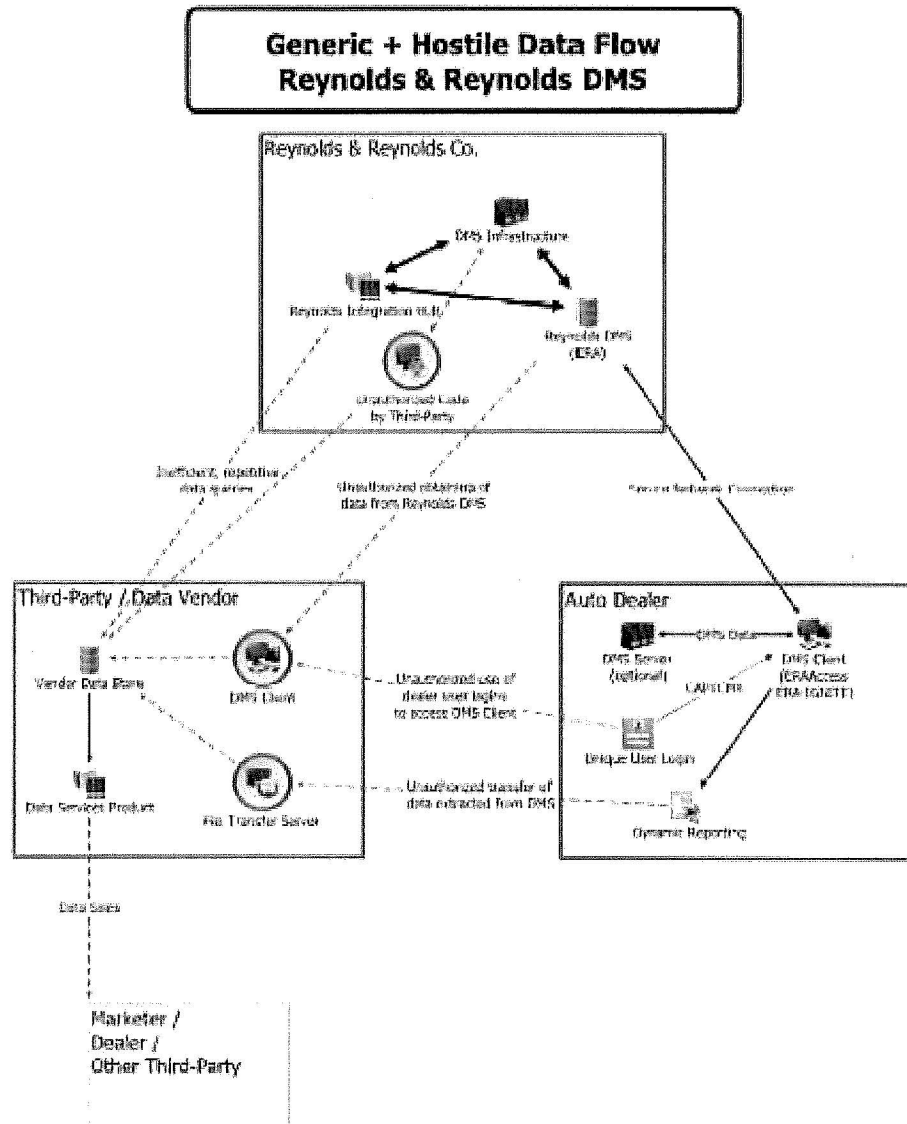
performed a memory “rip” of the Random Access Memory (RAM) of the local machine. The VICTIM did not know whether the memory read was conducted on the dealer’s device running the ERA-IGNITE thin client, the dealer’s server, or on the ERA-Server. The extracted answer from RAM would then be programmatically input to the CAPTCHA prompt.

26. Should the notepad.exe function fail, the PCM script would then execute CaptchaSolver.exe. The executable would take a screenshot of the screen displaying the CAPTCHA prompt, snip the window containing the prompt, and send the CAPTCHA question to Eastern European “CAPTCHA farm”. The SUBJECT COMPANY would pay the CAPTCHA farm tenths of a cent for each correct CAPTCHA answer.

27. When the CAPTCHA question was answered successfully, either through notepad.exe or CaptchaSolver.exe, the report was generated and exported back to the SUBJECT COMPANY virtual server for the cleaning and processing. According to depositions in the DMS Antitrust Litigation in 2018 from the Northern District of Illinois Eastern Division, on or about September 17, 2016, the SUBJECT COMPANY stated this cleaning and processing may have been accomplished through a “Spider Logic Database”, however, the VICTIM does not have further information on the process. The cleaned data was sent to DealerVault, the SUBJECT COMPANY owned program to house the datasets. The SUBJECT COMPANY then sold access to DealerVault and labeled it as their own DMS. The SUBJECT COMPANY’s data exfiltration and data processing is depicted in Figure 4.



Figure 4: Data flow between Authenticom, a dealership, and THE VICTIM DMS



29. Upon successful login to ERACCESS by an Authenticom user, the PCM script would navigate through the terminal window, exploiting the keyboard driver of the dealer PC using a PS2 emulator. Naturally, for both ERACCESS and ERA-IGNITE, the programs



prohibited the use of “SendKeys.” SendKeys is a function in windows that will send a keystroke to an active window.

30. In order to circumvent the security measure, the SUBJECT COMPANY would first convert the keystrokes into “scan codes” or machine level values representing a keystroke. Through this process, the SUBJECT COMPANY had the ability to simulate a user navigating the ERACCESS terminal or the ERA-IGNITE menus.

31. The SUBJECT COMPANY’s exfiltration of the VICTIM’s ERA-Servers occurred at various intervals, depending on the desired datatype. For example, datatypes that were sensitive were exfiltrated hourly. At certain intervals, the SUBJECT COMPANY would modify system logs on the DMS client to remove the queries conducted by an Authenticom profile. The DMS would then archive those modified logs in an archival system located on the DMS.

32. According to the deposition of Chris KIRBY in the DMS Antitrust Litigation in 2018 from the Northern District of Illinois Eastern Division, on or about September 17, 2016, Chris KIRBY and Brian CLEMENTSs exchanged an email with subject line “Operations Update.” Chris KIRBY testified the email referred to the SUBJECT COMPANY’s migration from Rackspace to Microsoft Azure.

33. On or about May 29, 2021, the VICTIM received a spreadsheet through the eDiscovery process of the DMS Antitrust Litigation from the Northern District of Illinois Eastern Division. The spreadsheet detailed the SUBJECT COMPANY’s Microsoft Azure SUBJECT ACCOUNT information, including, but not limited to: Account Owner ID, Account name, Subscription ID, Products purchased, Meter Category, Instance ID, and what appeared to be Virtual Machine META data.

**Security Updates from the VICTIM**

34. Prior to 2006, the DMS was owned by a different DMS provider. Business was conducted via Telnet over direct modem access, and third-party vendors freely scraped data from the DMS. However, after the VICTIM acquisition in 2006, the VICTIM barred non-licensed users from accessing the DMS.

35. In or around May, 2015, the below list, seen in Table 1, describes the VICTIM's updates and impacts observed by the SUBJECT COMPANY, which were emailed to Heidi DEARMAN, Russel GENTRY, Pam LANG, Brian CLEMENTS, Katie WIERSGALLA, Sarah GRAF, Joe NOTH, Roxane JERRICKS, Josh OELTJAN and from Noah M. LA LIBERTE.

Table 1: Authenticom's timeline of response and impact from THE VICTIM  
Security Updates

Start Date	Description	Count of affected Profiles
June, 2009	"R&R began prompting for Challenge questions"	~100% of RR profiles at the time
January, 2010	"R&R removed modem access"	~200 Profiles
May, 2010	"R&R began prompting for ASCII Captcha"	~90% of RR profiles at the time
January, 2012	"R&R replaced Telnet w/ encrypted SSH Port, ERAccess direct, Serial Number check"	~100% of RR profiles at the time
February, 2012	"R&R started disabling report generator profiles"	~300 profiles
May, 2013	"R&R began prompting Graphical CAPTCHA"	~100 profiles
June, 2013	"R&R again disabling Report Generator profiles"	~4000 profiles multiple times
April, 2014	"R&R presented RTS Challenges"	~75 profiles
September, 2014	"R&R again disabling Report Generator Profiles"	~80 profiles

March, 2015	“R&R again disabling report Generator Profiles”	~650 profiles
May, 2015	“R&R began disabling Dynamic Reporting Profiles”	~500 profiles

36. Many of the security updates implemented by the VICTIM were derived from heuristic analyses conducted by forensic teams. One of the methods discovered through heuristic analysis was the SUBJECT COMPANY logged into the DMS, created a new profile, sometimes utilizing a moniker with a variation of the word the SUBJECT COMPANY (e.g., “AuthenticomID”). The new profile would run a dynamic report, export the report (after successful CAPTCHA answer), then delete the report and profile.

37. Additional heuristic analysis and verbose logging pointed toward automated menu-walking events, suspected to be utilized to keep the session active. The VICTIM was able to ascertain the SUBJECT COMPANY’s activity due to menu walking occurring repeatedly in regularly timed intervals. In response, the VICTIM disabled the UserIDs temporarily or prevented them from performing Dynamic Report exports.

38. According to William MUNNS’s deposition, Software Engineer for the SUBJECT COMPANY, deposition in the DMS Antitrust Litigation in 2018 from the Northern District of Illinois Eastern Division, the SUBJECT COMPANY had 430 instances of THE VICTIM DMS active at the time of testimony, which was approximately December 2018. The SUBJECT COMPANY generally utilized a one-to-one relationship with those instances, meaning they had a virtual server hosting 2003 Windows server and their custom PCM script per dealer.

## **Piracy**



39. According to the VICTIM, the SUBJECT COMPANY has hosted copies of ERACCESS and/or ERA-IIGNITE on the SUBJECT COMPANY's virtual servers. ERACCESS or ERA-IGNITE would only be available for download via the Software Manager application provided to the dealer by the VICTIM. The VICTIM believed the SUBJCET COMPANY acquired a copy through the Software Manager application on the Dealer's PC. Steve COTTRELL, CEO of the SUBJECT COMPANY; Brian CLEMENTS, COO of the SUBJECT COMPANY; and William MUNNS from the 2018 -2019 DMS Litigation from the Northern District of Illinois Eastern Division purported in their depositions they had authorization to access the DMS due to permission granted by the authorized dealers.

40. Upon login to the DMS, the user is faced with a warning banner that states the following:

*NOTICE: YOU ARE ABOUT TO ACCESS CONFIDENTIAL AND PROPRIETARY INFORMATION*

*This software is proprietary property of the Reynolds and Reynolds Company and its affiliates ("Reynolds"), and its Licensors, copyright 1986-Present, all rights reserved.*

*This software is licensed not sold and is governed by the terms of the applicable agreement(s) with Reynolds. This software may not be copied, disclosed, decompiled, disassembled, shared with or accessed by a third party electronically or manually. It cannot be transferred or used except in accordance with the terms of the applicable agreement(s) with Reynolds. (Figure 1)*

41. Although William MUNNS admitted having seen the banner each time of successful or attempted login in his deposition from the 2018 -2019 DMS Litigation from the Northern District of Illinois Eastern Division, he could not say for certain to have downloaded the ERACCESS or ERA-IGNITE thin client onto any of the SUBJECT COMPANY device.

42. However, on or around October 2013, William MUNNS sent an email to CLEMENTS, Luke DOBBINS, Heidi DEARMAN, Kevin ANDERSON, and David MCDONALD stating "Every server that's picked up in the last 4 hours is on the newest version,

yet we're seeing lockouts. This tells us that we're no longer seeing update revisions, so theoretically ERA could be identifying phonies based on version incompatibility between the server and the dealer's system." William MUNNS suggested they "revert the ERACCESS executable on a number of our servers to the 9/4/2013 release (We have 21 now on 9/4, 397 on 9/23, I think we'd want at least 100 9/4 exes.)[Emphasis added]" and "Stop updating ERACCESS via PCM. PCM has a SystemOption called 'UpdateEraccess' that's supposed to not update when set to 0. This not working."

#### **Authenticom Collaborators**

43. Correspondence provided by the SUBJECT COMPANY to the VICTIM in the Dealer Management Systems Antitrust Litigation in 2018 from the Northern District of Illinois Eastern Division during eDiscovery suggested the SUBJECT COMPANY collaborated with other data brokers to find ways to circumvent the DMS security.

44. In or around September 2016, Brian CLEMENTS exchanged emails with Dave LAMPERT an employee of InDesign/1DMS. The two appeared to discuss solutions on how to prevent "Reynolds user shut offs." Brian CLEMENTS asked Dave LAMPERT a list of technical questions, such as: "What operating system are you using in Virtual Box (VM)," "Show us how to fix a broken installer?", "Show us some RAW data from the DMS before it is converted to JSON."

#### **Dissemination of Consumer Data**

45. In or around April 2019, Travis ROBINSON testified he was a shareholder for Data Services, LLC. Data Services, LLC was a data broker that took automotive data and sold it to third parties. The data sold by Data Services, LLC included data that the SUBJECT



COMPANY exfiltrated from the DMS. One of the other data companies Data Services, LLC sold to was Infutor Data Solutions, Inc.

46. In or around April, 2009, Steve COTTRELL, on behalf of Data Services, LLC, and Gary WALTER, President of Infutor Data Solutions, Inc., signed a Data License Agreement where, “INFUTOR obtains information describing transactions made by consumers and businesses in the United States, and maintains this information in computerized databases (“INFUTOR” Databases”); and DATA SERVICES procures, compiles, licenses, and maintains a proprietary computerized database including updates thereto (“DATA SERVICES Data”) composed of names and addresses of individuals and or businesses and related information...”

47. In or around December, 2011, Travis ROBINSON, exchanged letters with Wipfli LLP to purchase a web-based, client-facing database application to aid in the ingestion and aggregation of data from the auto dealer and service market that was provided to marketing companies, who for example, performed follow-ups on vehicle purchases and service appointments via phone calls, emails and letters to promote other offerings for purchase. The databases’ function was to sell end user data collected and sold to its clients, which are the marketing firms. This data can include sales, service, and inventory information along with customer data, keyed to VIN numbers.

**Damage Report by Daniel L. Rubinfeld**

48. On August 26, 2019, Daniel L. RUBINFELD, an American Economist, submitted expert damages report as part of a counterclaim from the VICTIM directed toward the SUBJECT COMPANY. Daniel L. RUBINFELD stated efforts to protect the DMS from unauthorized third-party access, including the cost of investigating and responding to such access and developing additional technological measures to protect DMS would be the same whether there was one or

many unauthorized users. According to the VICTIM, the SUBJECT COMPANY represented a significant percentage of the unauthorized access to the DMS. The costs would likely not have been spent if there were no hostile unauthorized access by third parties, such as the SUBJECT COMPANY.

Task	2013	2014	2015	2016	2017	2018	2019	Total
Data Services	\$ 385,639	\$ 410,441	\$ 315,591	\$ 281,832	\$ 206,802	\$ 190,307	\$ 125,885	\$1,916,497
Development	\$ 355,831	\$ 394,375	\$ 352,518	\$ 328,787	\$ 337,244	\$ 355,800	\$ 340,029	\$2,464,583
Quality Assurance	\$ 34,949	\$ 33,592	\$ 28,759	\$ 28,874	\$ 12,719	\$ 12,779	\$ 12,779	\$ 164,452
Technical Assistance	\$ 87,404	\$ 89,804	\$ 381,290	\$ 510,216	\$ 502,435	\$ 339,173	\$ 221,304	\$2,131,636
<b>Total</b>	<b>\$ 863,823</b>	<b>\$ 928,212</b>	<b>\$1,078,159</b>	<b>\$1,149,719</b>	<b>\$1,059,199</b>	<b>\$ 898,059</b>	<b>\$ 699,997</b>	<b>\$6,677,169</b>

**Table 2: Estimated Costs for Monitoring and Preventing unauthorized access to DMS by Rubinfeld**

49. As shown in Table 2, RUBENFELD estimated a dollar loss of approximately \$6,677,169. However, the VICTIM records of the SUBJECT COMPANY's automated access to its system was incomplete, and the VICTIM was not able to specify the exact percentage of unauthorized access to its system by the SUBJECT COMPANY over time. Therefore, the VICTIM held the position \$6,677,169 to be a conservative, lower number than actual damages.

50. As shown in Table 2, RUBENFELD estimated a dollar loss of approximately \$6,677,169. However, the VICTIM records of the SUBJECT COMPANY's automated access to its system was incomplete, and the VICTIM was not able to specify the exact percentage of unauthorized access to its system by the SUBJECT COMPANY over time. Therefore, the VICTIM held the position \$6,677,169 to be a conservative, lower number than actual damages.

51. On August 6, 2021, A review of Microsoft Azure records revealed the subject's use of SQL servers, server farms for large data storage, and Virtual Machines matching the descriptions from discovery documents.

52. On March 22, 2022, a review of Microsoft Azure records identified two likely IP addresses associated with a Microsoft Azure virtual server hosting the polling script: 40.79.75.192 and 157.56.164.15.

53. Microsoft has confirmed that the SUBJECT COMPANY still maintains infrastructure on Microsoft Azure through the SUBJECT ACCOUNT.

**CONCLUSION**

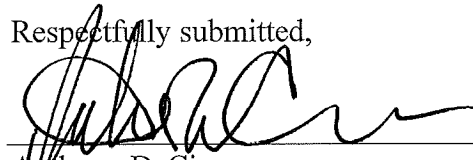
54. Based on the forgoing, I request that the Court issue the proposed search warrant.

55. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Microsoft Corporation. Because the warrant will be served on Microsoft Corporation who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

**REQUEST FOR SEALING**

56. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

  
\_\_\_\_\_  
Anthony DeCicco  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on June 22, 2022

  
\_\_\_\_\_  
Caroline H. Gentry  
United States Magistrate Judge





**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to records and information associated with Microsoft Azure account: with cloud service assigned with chrisk[@]lac.authenticom.com and Microsoft Azure Active Directory IDs: 501d2bc4-5948-40e9-ad5e-f1f4ee3718f2, 91845580-9c09-41e0-82fa-feec820216ed, a0285d75-854d-4fde-9e8e-45c3d2800285, 78807487-964f-4c90-8647-e55ce75705a7 and 74b34da8-d8b7-423a-af50-e5b27cce2d5f (“the SUBJECT ACCOUNT”), with listed subscriber(s) **Authenticom LLC**, or that is in the custody or control of **Microsoft Azure**, a cloud service provider that is headquartered at **1 Microsoft Way, Redmond, WA 98052**. As a provider of cloud services, **Microsoft** is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15).

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Microsoft Corporation**

To the extent that the information described in Attachment A is within the possession, custody, or control of Microsoft Corporation, including any messages, records, files, logs, or information that have been deleted but are still available to Microsoft Corporation, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(e), Microsoft Corporation is required to disclose the following information to the government for each account or identifier listed in Attachment A from time period of Jan. 1, 2021 to the present:

- a. all records or other information pertaining to that account or identifier, including all virtual disks, files, databases, and database records stored by Microsoft Corporation in relation to that account or identifier;
- b. all information in the possession of Microsoft Corporation that might identify the subscribers related to those accounts or identifiers, including names, addresses, telephone numbers and other identifiers, e-mail addresses, business information, the length of service (including start date), means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;
- c. all records pertaining to the types of service utilized by the user,
- d. all records pertaining to communications between Microsoft Corporation and any person regarding the account or identifier, including contacts with support services and records of actions taken.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 1030(A)(5)(a) involving Authenticom since November 2018, relating to the development, publishing, advertisement, access, use, administration or maintenance of any online service or digital code enumerated in Attachment A, including:

1. Contents for a virtual machine, which may include, but is not limited to Microsoft Windows Server 2003 Operating system, used to facilitate the intrusion;
2. Files, databases, and database records stored by Microsoft Corporation on behalf of the subscriber or user operating the sever, including:
  - a. Any computer code, including computer scripts and compiled programs used to serve or process requests made via any network communication protocol, facilitate access to a computer system, exploit vulnerabilities in a computer system;
  - b. Log files created by any computer program or service that might contain evidence of unauthorized access to any computer system or network;
  - c. Logs showing connections to and from the server, and any other transactional information, including records of session times and durations, log files, dates and times of connecting, methods of connecting, and ports;

- d. Digital software, computer code, or scripts designed to: exploit vulnerabilities in, facilitate unauthorized access to, circumvent access controls such as passwords encryption keys or digital certificates for, or steal information from any computer hardware, software, network, or communications protocol.
  - e. MySQL, PostgreSQL, or other databases related to the virtual machine;
  - f. email accounts and the contents thereof, associated with the account.
3. Subscriber information related to the accounts established to host the site

enumerated in Attachment A, to include:

- a. Names, physical addresses, telephone numbers and other identifiers, email addresses, and business information;
- b. Length of service (including start date), types of service utilized, means and source of payment for services (including any credit card or back account number), and billing and payment information;
- c. A list of all IP addresses assigned to the server, along with the dates and times for which such IP's were assigned.
- d. If a domain name was registered on behalf of the subscriber, the date that the domain was registered, the domain name, the registrant information, administrative contact information, the technical contact information and billing contact used to register the domain and the method of payment tendered to secure and register the Internet domain name.